REMARKS

Reconsideration of the rejections set forth in the Office Action dated September 20, 2006 is respectfully requested. By this amendment claims 13 and 15 have been amended. Currently, claims 1-7, 9-11, and 13-25 are pending in this application.

Objection to the claims

The Examiner objected to claims 13 and 15 for reciting improper dependencies. Applicants have amended the dependencies of these claims and respectfully request that the objection be withdrawn.

Rejection under 35 USC 103 over Hamilton and Amara

Claims 1-3, 7, 9-11, 13-15, and 17-22 were rejected under 35 USC 103 as unpatentable over Hamilton (U.S. Patent No. 7,123,974) in view of Amara (U.S. Patent Application Publication No. 2004/0082395). This rejection is respectfully traversed in view of the amendments to the claims and the following arguments.

This application relates to industrial networks, and more particularly to a way in which access to particular PLCs and attendant factory machines may be circumscribed so that only particular authorized individuals may have access to particular PLCs. As discussed in the background of the specification, for example at page 1, PLCs are able to be connected to a company's Ethernet network or other data network. However, where there is more than one person that is allowed to program PLCs on the network, a person may accidentally make a change to the wrong PLC or a person may intentionally change the programs of PLCs on the network to affect operation of the machines associated with the PLCs. Accordingly, applicants proposed to implement a security point (Secure Policy Implementation Point – SPIP) between the network and the PLC to control who is allowed to access particular PLCs on the network. Thus, simply obtaining access to a centralized network controller is insufficient to program all PLCs connected to the network – the SPIP will also require that the user of the network control system be authenticated and authorized before allowing the user to make changes to the PLC control program.

As described at page 9, line 27 to page 10, line 6, the SPIP is configured to participate in a Virtual Private Network (VPN) such that communications with the SPIP over the industrial network occur over a VPN tunnel. This prevents unauthorized individuals from viewing and/or modifying the communications between the SPIP and the central control or other network devices, and also enables other sundry benefits attendant to VPNs to be implemented in connection with programming PLCs.

Hamilton teaches a way in which changes to a PLC may be recorded. Specifically, Hamilton teaches that PLCs (industrial control components 24) may be accessed by an access tool 20 via a network 30 (Col. 4, lines 60-61). Hamilton does not address how access the tool may be controlled or how the path between the access tool 20 and the industrial control components 24 may be secured, but rather focuses on how any changes to the industrial control components 24 may be recorded. (See, e.g., Hamilton at Col. 5, lines 4-23 – describing types of actions that may be logged, and Col. 4, lines 19-23 – describing invention as "a system and methodology facilitating automated audit recording and tracking of PLC-based interactions.").

The way in which Hamilton records changes to the PLC, is by implementing a recording component 40 that logs the changes to the PLC, and a tracking component 44 that stores the information collected by the recording component in a database. (Col. 5, lines 24-42). These components may be implemented in the access tool 20 (See Fig. 1 elements 40 and 44 in Access tool 20) or in the PLCs themselves (See Fig. 2 element 170 in client system (PLCs) 124, see also Col. 6, lines 6-23). Data stored by the recording and tracking component 170 is stored as data 180 in a database 174. (Col. 6, lines 23-43). To access the data 180 that has been recorded by the recording and tracking component 170, the user is required to perform a login procedure with the tracking component 170 to determine whether a user of the application 144 has the authority to access the data 180. (Col. 6, lines 43-48).

Hamilton does not address how access to a PLC should be controlled. Specifically, Hamilton does not teach or suggest "a security policy implementation point (SPIP) connected between the local area network and the one or more programmable logic controllers to isolate the one or more programmable logic controllers and associated factory machines from the local area network" as recited in claim 1. Rather, Hamilton allows anyone to program the PLC and simply records the events that are occurring at the PLC. The recorded data is then protected from being accessed, but the underlying PLC itself is not protected. Rather, the PLCs are connected directly to the local area network so that the PLCs are accessible to any user that has obtained access to the network. Stated differently, since the PLCs are directly connected to the network, there is no SPIP implemented intermediate the network and the PLCs to control access to the PLCs.

The Examiner cited Fig. 6, and the text at Col. 9, lines 7-33 of Hamilton as teaching a SPIP connected between the network and the one or more PLCs to isolate the PLCs from the network. Fig. 6 of Hamilton shows an access tool 510 having one or more security layers 520. Referring back to Fig. 1, the access tool 20 is the component that is used to interact with the PLCs via the network 30. Fig. 6 thus shows that it is possible to implement security in the management station so that communications on the network are secured. This would require a user to log into the management station to be able to adjust operating parameters of the PLCs. This does not show, however, that SPIPs should be deployed "between the local area network and the one or more programmable logic controllers" as claimed.

Applicants acknowledged in the background of the application that PLCs could be accessed over the network using existing management programs (Specification at Page 1, lines 23-29). Hamilton teaches one such program that may be used to track modifications to the PLCs. It uses standard login procedures to control access to the data that is logged from the PLCs. Hamilton does not teach or suggest, however implementing a second layer of control in the form of an SPIP between the PLC and the network that will prevent someone using a management program from having access to particular PLCs.

On page 3, lines 2-4 of the Office Action, the Examiner states that Hamilton teaches a SPIP connected between the network and the one or more PLCs. However, later on the same page (page 3, lines 8-11) the Examiner concedes that Hamilton "doesn't expressively mention, the SPIP connected between the local area network and the one or more programmable logic controllers and, a VPN tunnel." The Examiner then cites Amara as teaching a SPIP connected between the local area network and one or more PLCs (which the Examiner contends are shown in Amara as computers, switches, routers, servers, and gateways.) (Office Action at page 3, lines 12-14).

First, applicants respectfully submit that a personal computer, laptop computer, mobile phone, PDA and access server shown in Fig 1 as connecting to the network backbone 120 are not PLCs, as that term is used in this application. See Specification at page 1, lines 13-16, in which PLCs are defined as small programmable devices that allow the operation of the factory machines to be altered. See also Specification at Page 5, lines 4-5 describing PLCs as devices that receive inputs from the factor machines and/or external sensors, and control the operation of the factory machine. Thus, Amara does not teach or suggest a SPIP between a PLC and a network.

Second, Amara does not teach SPIPs intermediate a network and the various computers/handheld devices. For example, in Fig. 1 of Amara, the initiating security gateway 140 is implemented on the network backbone 120 between a home agent 130 and a terminating security gateway 180. The network backbone is an ISP network (see Amara at Par. 38) through which a user may obtain connectivity to the network 170. Thus, the security layer in Amara exists between the ISP network and the terminating security gateway 180. Additionally, the user devices 102-108 of Amara are configured to implement IPSec, L2TP, or PPTP to secure the connections between the devices 102-108 and the home agent 130. Accordingly, since these devices themselves are computers or computer like devices capable of implementing the tunneling mechanisms, there would be no need in Amara to implement an SPIP between the devices 102-108 and the home agent 130.

Thus, it appears to applicants that Hamilton teaches that PLCs may be connected to a network and that changes to the PLC may be logged to determine how a PLC program has changed over time. Amara teaches a network in which ordinary network devices such as computers, rather than PLCs, are allowed implement tunnels to a home agent using one of a number of standard tunneling protocols.

Applicants respectfully submit that the combination of these would not result in the claimed combination. Specifically, Hamilton does not teach or suggest using a SPIP intermediate a network and a PLC – the Examiner has conceded this point. Amara, similarly, does not teach or suggest using a SPIP intermediate a network and a PLC because (1) the devices in Amara are not PLCs, and (2) the devices in Amara are sufficiently powerful to perform tunneling themselves. Thus, there is no need to implement an SPIP intermediate the network and the devices of Amara. Accordingly, since both Hamilton and Amara fail to teach or suggest a SPIP intermediate an end device such as a PLC and the network, the combination of Hamilton and Amara does not render claim 1 obvious.

Moreover, the SPIP of claim 1 does more than merely implement a tunnel. Rather, claim 1 states that the SPIP is configured "to isolate the one or more programmable logic controllers and associated factory machines from the local area network". There is nothing in Amara or

Hamilton that teaches or suggests isolating individual PLCs from the rest of the network. Accordingly, for this additional reason, applicants respectfully submit that the combination of Hamilton and Amara would not have made the invention recited in claim 1 obvious.

Rejection under 35 USC 103 over Hamilton, Amara, and Danner

Claims 4-6 and 23-25 were rejected under 35 USC 103 as unpatentable over Hamilton in view of Amara, and further in view of Danner (U.S. Patent Application No. 7,194,003). The claims rejected under this combination of references are dependent claims and, as such, are patentable for at least the reasons set forth above in connection with the independent claims.

Conclusion

In view of foregoing remarks, it is respectfully submitted that the application is now in condition for allowance and an action to this effect is respectfully requested. If there are any questions or concerns regarding the amendments or these remarks, the Examiner is requested to telephone the undersigned at the telephone number listed below.

If any fees are due in connection with this filing, the Commissioner is hereby authorized to charge payment of the fees associated with this communication or credit any overpayment to Deposit Account No. 502246 (Ref: NN-15929).

Respectfully Submitted

John C Gorecki

John C. Gorecki
Registration No. 38,471

Dated: August 27, 2007

John C. Gorecki, Esq.
P.O. Box 553
Carlisle, MA 01741
Tel: (978) 371-3218
Fax: (978) 371-3219
john@gorecki.us